IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF: 13159 LAKEHILL DRIVE NOKESVILLE, VIRGINIA 20181 AND 8870 RIXLEW LANE, SUITES 201 AND 204, MANASSAS, VIRGINIA 20109	**Filed Under Seal** No. 1:21-sw-279 No. 1:21-sw-280

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Robert Valdini, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 13159 Lakehill Drive, Nokesville, VA 20181 (RESIDENTIAL PREMISES) and the premises known as 8870 Rixlew Lane, Suite 201 and 204, Manassas, Virginia 20109 (OFFICE PREMISES) further described in Attachments A, for the items described in Attachment B.

2. I am a Special Agent with the Internal Revenue Service, Criminal Investigation ("IRS-CI") and have been so employed since August 2011. As a Special Agent, my duties and responsibilities include conducting investigations of potential violations of the United States Code including Title 26 (Internal Revenue), Title 18 (Money Laundering and other Federal crimes), and Title 31 (Bank Secrecy Act). I have also assisted in investigations of other Title 18 violations including bankruptcy fraud and wire

fraud. I received training in the laws of search and seizure and in the use of search warrants in tax-related investigations during a six-month training program at the Federal Law Enforcement Training Center ("FLETC") in Brunswick, Georgia.

3. As a federal agent, I am authorized to investigate violations of laws of the United States, and as a law enforcement officer I am authorized to execute warrants issued under the authority of the United States.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. Particularly I have consulted a special agent with the FBI who is working this case jointly with me. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of 18 U.S.C. § 1343 (wire fraud), 1957 (transactions with criminal proceeds); 18 U.S.C. § 157 (bankruptcy fraud); 26 U.S.C. § 7201 (attempt to evade or defeat tax); and 26 U.S.C. § 7203 (willful failure to file return or supply information) have been committed and that evidence of those violations exists at both PREMISES. Thus, there is probable cause to search both PREMISES, further described in Attachment A, for the items described in Attachment B.

BACKGROUND

6. This investigation involves a subject who is a non-attorney partner in a business registered in the District of Columbia and which operates out of Manassas,

Virginia. As explained further below, there is probable cause to believe that the subject may have violated federal law concerning wire fraud, bankruptcy fraud, the failing to file tax returns, and the assessment and payment of taxes. There is also probable cause to believe that evidence of this criminal activity may be found within both PREMISES to be searched.

7. DAVID MARESCA (SSN: xxx-xx-7503) is forty-six years old and has an address at 13159 Lakehill Drive Nokesville, Virginia. MARESCA has failed to file his federal tax returns for at least tax years 2017, 2018, and 2019. MARESCA is a principal for several different companies.

8. Records provided by a third-party showed SYNERGY ATTORNEY SERVICES LLC ("SAS") was incorporated in the Commonwealth of Virginia effective April 27, 2015. MARESCA is listed as the sole member with 100% ownership interest.

9. According to records provided by the Government of the District of Columbia, Department of Consumer and Regulatory Affairs Corporations Division ("DCRA"), SYNERGY LAW LLC ("SYNERGY")[1] was a business incorporated in the District of Columbia. The Articles of Organization for SYNERGY were transmitted to the DCRA in Washington, D.C., via interstate wires on or about October 17, 2016. SYNERGY also transmitted a Two-Year Report for Domestic and Foreign Filing Entity to the DCRA via the interstate wires on or about October 26, 2017. SYNERGY's certificate and registration was revoked on or about September 12, 2019.

---

[1] Although MARESCA is a partner in SYNERGY, MARESCA is not nor ever was an attorney. In the District of Columbia, a non-attorney may be a partner in a law firm.

10. SYNERGY filed for bankruptcy in U.S. Bankruptcy Court for the District of Columbia on or about August 16, 2019. The business was incorporated by MARESCA, and according to his testimony provided at a meeting of creditors on October 18, 2019, MARESCA was a 90 percent shareholder in SYNERGY. The remaining 10 percent of SYNERGY was owned by SCOTT MARINELLI, a member of the D.C. Bar whose license to practice law was suspended in or about May 2018.

11. Records provided by the Commonwealth of Virginia State Corporation Commission show SYNERGY STAFFING LLC was a business incorporated in the Commonwealth of Virginia effective April 11, 2019. MARESCA was the corporation's registered agent and organizer, and listed the company's initial registered office, which was identical to the business office of the registered agent, as 13159 Lakehill Drive, Nokesville, Virginia 20181 ("RESIDENTIAL PREMISES"). The company's principal office where the records of the company were to be kept was listed as 8870 Rixlew Lane, Suite #201, Manassas, Virginia 20109 ("OFFICE PREMISES").

12. Records provided by the DCRA show THEMIS LAW LLC ("THEMIS") was a business incorporated in the District of Columbia. The Articles of Organization for THEMIS were transmitted over the interstate wires to the DCRA in Washington, D.C., on or about June 20, 2019. The certificate and registration for THEMIS was revoked September 17, 2020. The business organizers are listed as MARESCA and SAM BABBS III.

13. SAM BABBS III is an attorney admitted to the Florida Bar on September 25, 2008, and the District of Columbia Bar on August 10, 2009.

14. According to MARESCA's October 18, 2019, testimony provided at a 341 Meeting of Creditors before the U.S. Bankruptcy Court for the District of Columbia, SYNERGY STAFFING pays the THEMIS employee salaries and was initially set up to provide employees for SYNERGY for a fee. MARESCA also testified that SYNERGY STAFFING is paid by THEMIS for those services.

15. As discussed in more detail below, SYNERGY filed for bankruptcy in the District of Columbia in 2019. Approximately two months prior to filing for bankruptcy, MARESCA incorporated THEMIS, and all of SYNERGY's assets were transferred to THEMIS for no consideration. MARESCA testified at a 341 Meeting of Creditors before the U.S. Bankruptcy Court for the District of Columbia on October 18, 2019, that his name is personally on the lease for the OFFICE PREMISES and that THEMIS took over occupancy of that space from SYNERGY. Additionally, many of the former SYNERGY employees became THEMIS employees, and a majority of the SYNERGY clients were transferred to THEMIS. The only difference in the operation of THEMIS from SYNERGY besides the name, was that the remaining 10 percent was owned by BABBS rather than MARINELLI.

16. MARESCA personally filed for Chapter 11 bankruptcy in the Eastern District of Virginia in 2020. During the course of the bankruptcy proceedings, MARESCA submitted to the bankruptcy court three personal tax returns for tax years 2017, 2018, and 2019, that MARESCA alleges that he filed with the IRS. The returns were self-prepared and dated January 8, 2021. MARESCA also stated that he had filed the tax returns for SYNERGY and THEMIS with the IRS. As of April 5, 2021, there are no records with the

IRS that indicate that any such returns were filed for MARESCA, SYNERGY, or THEMIS.

FORECLOSURE DEFENSE SCHEME

17. According to victim homeowners interviewed during this investigation, SYNERGY, and subsequently THEMIS, marketed itself as a nation-wide law firm that could help distressed homeowners stay in their homes. SYNERGY-THEMIS employees told distressed homeowners the "firm" was comprised of a team of highly successful attorneys and mortgage industry professionals who could negotiate loan modifications on the homeowner's behalf within six months.

18. Victim homeowners who retained SYNERGY-THEMIS's services made upfront payments in anticipation of receiving loan modification and foreclosure services from what the victims believed was a law firm, retained to represent them. To the contrary, very few of the victim homeowners interviewed ever spoke with an attorney and very few loan modifications were obtained on behalf of those homeowners. In reality, SYNERGY-THEMIS would consistently ask clients for the same information over and over again; consistently provide a new representative to work with the client; and would usually only reach out to the client at the end of the month to verify the processing of payment for "services" of SYNERGY-THEMIS.

19. Mortgage records reviewed during this investigation also showed that in some cases there were significant delays in SYNERGY-THEMIS contacting and providing the required loan modification documents to the mortgage companies and little to no action

taken by SYNERGY-THEMIS to renegotiate the mortgages. In other cases, the lender was never even contacted by SYNERGY-THEMIS.

20. When faced with foreclosure sales, several victim homeowners interviewed in this case were told by SYNERGY-THEMIS to file an initial bankruptcy petition to stop the sale of the property. Many of those victim homeowners were instructed by SYNERGY-THEMIS to complete and file bankruptcy petitions in U.S. Bankruptcy Court as an individual, omitting they had retained SYNERGY-THEMIS's services.

21. Many of the victim homeowners interviewed were elderly low-income individuals who were in desperate financial situations. Some of the victim homeowners include the following:

a. Client A, a forty-five-year-old Navy veteran, contacted THEMIS in approximately January 2019 for assistance to negotiate better terms and a lower interest rate for a home that they owed in Chesapeake, Virginia. Client A paid THEMIS $800 per month which was automatically charged to Client A's credit card every month. THEMIS told Client A that THEMIS could save Client A's house and get Client A better interest rate, and THEMIS would deal directly with the mortgage company on behalf of Client A. Client A emailed THEMIS a number of documents. Approximately seven months later in July 2019, Client A's spouse called the mortgage company and was told that THEMIS had never contacted them. Client A then contacted THEMIS and was told by a representative "they [the mortgage company] can tell you anything." Client A told the THEMIS representative she would stop

payment to THEMIS. The representative hung up on Client A and THEMIS continued to charge Client A's credit card.

b. Client B, a sixty-six-year-old government contract employee, contacted SYNERGY in early 2018, after she was unable to obtain a loan modification from her mortgage company for her house located in the District of Columbia. Client B stated that she was desperate to save her house and believed she was hiring a team of attorneys and industry experts to help her obtain a loan modification. Client B stated that SYNERGY was based in Manassas, Virginia. On May 31, 2018, Client B contacted SYNERGY telephonically and spoke to a representative who emailed Client B an application. The representative set up automatic payments to be debited from Client B's bank account. Client B was told by the representative that the automatic payments had to be set up. During this call Client B's first payment was debited. Client B stated that they paid a couple of thousand dollars in total to SYNERGY. Client B sent SYNERGY various documents in order for SYNERGY to negotiate a loan modification. Client B then contacted their mortgage company who told Client B that no one from SYNERGY had ever contacted the mortgage company. When Client B attempted to stop payments to SYNERGY, a representative from SYNERGY told Client B that they signed a contract and that SYNERGY would sue Client B if payments stopped. When Client B told SYNERGY that the mortgage company had not received any communication from

SYNERGY, the SYNERGY representative told Client B that the mortgage company was lying. SYNERGY refused to issue a refund to Client B.

c. Client C, a sixty-six-year-old retired disabled school teacher was telephonically contacted by THEMIS in September 2019. Client C did not know how THEMIS obtained her name and contact information. Client C was having difficulty paying her mortgage on her residence in the District of Columbia and the representative from THEMIS told Client C that THEMIS could help her get a loan modification. THEMIS's fee was approximately $600 per month. Client C was told by the THEMIS representative not to make any mortgage payments while THEMIS negotiated the loan modification. Client C sent THEMIS between 20-30 documents via mail and she also sent some faxes from a friend's residence in District Heights, Maryland. Client C also brought documents to THEMIS's office in Manassas, Virginia. THEMIS did not contact Client C with updates; THEMIS only called her regarding payments including while she was receiving dialysis treatment. In May 2020 Client C's loan modification was ultimately denied and Client C was approximately $17,000 behind on her mortgage and that if it was not paid the house would go into foreclosure.

22. Over the last several months, law enforcement conducted an undercover operation in which an FBI agent posed as a distressed homeowner attempting to forestall

foreclosure and to get a modification on their home loan. This operation corroborated many of the statements made by the victim homeowners to law enforcement.

23. During an unscheduled meeting at the THEMIS offices, the Undercover Employee ("UCE") met with multiple employees of THEMIS. In a meeting with an employee from client relations, the THEMIS employee told the UCE that THEMIS "tried to reach out to the lender multiple times" and that the lender would not cooperate, and the only option was to complete a short sale. The UCE was then told that the monthly fee that was paid by the UCE covered attorneys' fees but not the UCE's ability to speak to the attorneys. If there was an attorney on the case the fee would be an additional $500 per hour.

24. Ultimately, the UCE met with a person from the legal department. The employee from the legal department told the UCE that "I'm an attorney but paralegal here." During the course of the discussion this employee advised the UCE that if the UCE wanted to keep the residence, the UCE needed to file Chapter 13 bankruptcy or, in the alternative, the UCE should stop making mortgage payments and could live at the residence for six to nine months before the house was sold at which point the UCE could file for Chapter 7 bankruptcy and walk away.

25. During this investigation, law enforcement interviewed Employee 1 who is a former employee of SYNERGY. Employee 1 worked for SYNERGY for several months at the end of 2018 and the beginning of 2019 as a "closer." As a "closer" it was Employee 1's responsibility to walk potential clients through an eight-page script that was written by MARESCA. The script which had to be memorized by Employee 1, told the potential client that SYNERGY would help save their house from foreclosure. However, a key

component of the script was that SYNERGY could not start assisting the client until the retainer was paid. The retainer was set at between $700 and $1,500. Employee 1 stated that these calls would last approximately 45 minutes and the most important information gathered was the potential client's ability to pay the retainer. Employee 1 estimated that SYNERGY ultimately helped 30 percent of their clients in getting a modification. If the client's case was deemed hopeless, no work was performed by SYNERGY including not contacting the mortgage holders, but SYNERGY did string the clients along to continue to pay the monthly fees. Employee 1 stated that MARESCA was the person in charge of SYNERGY and had a hands-on approach including listening in on the phone calls of employees.

26. During this investigation, I have learned that SYNERGY-THEMIS collected more than $8 million in fees for purported services provided by the law firms. However, only a fraction of the firm's clients actually received legal services from licensed attorneys.

TRANSACTION WITH PROCEEDS OF CRIME

27. Between the years 2016 and 2018, SYNERGY maintained several bank accounts. During my investigation, I have learned that SYNERGY had an operating account at Capital One Bank (x-0777). MARESCA had signature authority for Account x-0777 which was opened on or about April 6, 2017. Account x-0777 received funds from SYNERGY's clients who falsely believed that SYNERGY was providing legal services to them.[2]

---

[2] Many SYNERGY clients made monthly payments to SYNERGY via LawPay, an online service that collects payment from law firm clients. LawPay aggregated funds due to

28. On or about May 24, 2018, MARESCA purchased a cashier's check drawn against Account x-0777 payable to Sunshine Title & Settlement, Inc. ("Sunshine Title"), in the amount of $150,000. That check was intended as the earnest deposit for the purchase of a property located at "13159 Lake Hill Drive" which is the RESIDENTIAL PREMISES. That earnest money was deposited into an account held by Sunshine Title on or about May 31, 2018.

29. On or about August 29, 2018, MARESCA closed on the purchase of the RESIDENTIAL PREMISES. At the closing, SUNSHINE TITLE credited the earnest money deposit towards MARESCA's purchase of the RESIDENTIAL PREMISES.

BANKRUPTCY FRAUD

30. It is a violation of federal law for any person willfully to obstruct a bankruptcy proceeding, to file a materially false document in a bankruptcy proceeding, or to make a bankruptcy filing in furtherance of a scheme or artifice to defraud. 18 U.S.C. §§ 152, 157, 1001, and 1519.

31. MARESCA filed two separate petitions for voluntary Chapter 11 bankruptcy. MARASECA filed for personal bankruptcy on June 19, 2020 in the Eastern District of Virginia and for SYNERGY in the District of Columbia on August 16, 2019. There is probable cause to believe that MARESCA has committed bankruptcy fraud in both matters.

Personal Bankruptcy in the Eastern District of Virginia

32. On January 25, 2021, MARESCA, through his bankruptcy attorney, filed

---

SYNERGY and periodically transferred those funds to SYNERGY's accounts with Capital One including Account x-0777.

an objection to an IRS proof of claim. The filing alleges that MARESCA had filed his 2017, 2018, and 2019 tax returns and that MARESCA self-prepared these tax returns. The tax returns were purportedly dated January 8, 2021.

33. On January 25, 2021, MARESCA testified at a hearing in the Eastern District of Virginia. MARESCA testified that he had filed his 2016 tax return and that all of his tax returns were current and filed. MARESCA also stated that the 2019 tax return for THEMIS was filed with the IRS, but MARESCA did not know if the THEMIS tax returns were correct.

34. That same day, MARESCA provided copies of these self-prepared tax returns to the bankruptcy court for the years 2017, 2018, and 2019. MARESCA also testified before submitting the tax returns to the bankruptcy court that MARESCA had worked with an accountant to prepare his tax returns. MARESCA testified that he hired an individual named "Sharine" to prepare the tax returns for THEMIS but in the middle of working on the returns, "Sharine" doubled their prices.

35. As discussed later in this affidavit, these self-prepared personal tax returns for 2017, 2018, and 2019 that MARESCA submitted to the bankruptcy court are fraudulent. In addition, as of April 5, 2021, there is no record of MARESCA filing these tax returns with the IRS. There is also no record as of April 5, 2021, that tax returns were filed for SYNERGY or THEMIS for tax years 2017, 2018, and 2019.

36. There is probable cause to believe that MARESCA has made other materially false statements and omissions in his personal bankruptcy. For example, MARESCA was required in filing for bankruptcy to disclose his ownership interests in any companies and in any bank accounts. MARESCA's filings with the bankruptcy court in

the Eastern District of Virginia failed to disclose his 100 percent ownership interest in SYNERGY STAFFING.

37. MARESCA also failed to disclose a position that he holds as the chairman of Grace and Truth International Church. In fact, MARESCA had signatory authority over the church's bank account. MARESCA's position with this organization was ultimately discovered by the U.S. Trustee's Office based on a search of public records. When MARESCA eventually discussed these matters with the bankruptcy court, MARESCA testified that he was responsible for the bookkeeping and accounting of the organization.

38. However, MARESCA told the bankruptcy court that the books and records of THEMIS are being kept by Angela Smith Crump, using QuickBooks. Based on victim interviews conducted during this investigation, Crump has been identified as an employee of THEMIS. Based on my training an experience, because businesses typically maintain records of their business activity at their offices, there is probable cause to believe that copies of the books and records for THEMIS will be maintained at the OFFICE PREMISES.

Corporate Bankruptcy in the District of Columbia

39. MARESCA, acting as "CEO/Majority Member," filed a Chapter 7 bankruptcy petition in the U.S. Bankruptcy Court for the District of Columbia on August 16, 2019.

40. As noted above, at a meeting of creditors in the Bankruptcy Court for the District of Columbia in October 2019, MARESCA testified that the assets of SYNERGY were transferred to THEMIS for no consideration and that MARESCA had the same 90 percent ownership of THEMIS as he had in SYNERGY. THEMIS was organized in the

District of Columbia in June 2019 approximately two months prior to SYNERGY's bankruptcy petition.

41. At the meeting of creditors in the District of Columbia, MARESCA testified that THEMIS used the same office space and employed many of the same employees as SYNERGY. A majority of the clients of SYNERGY became clients of THEMIS.[3]

42. MARESCA further testified that SYNERGY was the subject of multiple investigations in various states. Claims and judgements were filed against SYNERGY for a multitude of reasons including for unauthorized practice of law, failure to disclose petition preparer fees, and failure to deliver bankruptcy services promised to clients for which clients paid. Disgorgement orders, civil penalties, and injunctions have been issued against SYNERGY in various states. MARESCA also admitted that SYNERGY had not filed federal income taxes for at least tax years 2017, 2018, and 2019.

43. During this investigation, I have learned that in or about April 2019—just four months prior to filing for bankruptcy—SYNERGY entered into an agreement with a company called Smart Business through which SYNERGY sold $446,970 worth of future receivables to Smart Business in exchange for a lump sum payment of $300,000 ("Receivables Agreement").[4] The Receivables Agreement allowed Smart Business to debit $4,299 every day from SYNERGY's bank account at Capital One. As part of the

---

[3] Law enforcement has learned in this investigation that THEMIS operated in the same vein and provided the same purported services that SYNERGY did. The only true difference between SYNERGY and THEMIS other than the name was that the attorney serving as a 10 percent partner had changed from MARESCA to BABBS.

[4] My statements related to the Receivables Agreement are based on a verified civil complaint filed against SYNERGY and MARESCA in the Supreme Court of the State of New York for Nassau County. *Smart Business v. Synergy Law, LLC, et al.*

Receivables Agreement, SYNERGY and MARESCA confessed judgment in the full amount due to Smart Business plus the costs of collection in the event that SYNERGY and MARESCA breached the Receivables Agreement.

44. I have also learned that on or about June 12, 2019, SYNERGY breached the Receivables Agreement. Smart Business had a judgment entered against SYNERGY in New York State court on that same day in the amount of $343,657.60 ("Receivables Judgment") which was the amount of money still due to Smart Business under the Receivables Agreement plus the costs of collection including attorney's fees.

45. I have further learned that entry of the Receivables Judgment, SYNERGY and Smart Business negotiated a second agreement by which Smart Business would forego collection on the Receivables Judgment in exchange for SYNERGY agreeing to pay some of the money due to Smart Business on an agreed-upon schedule ("Forbearance Agreement"). The Forbearance Agreement was finalized on or about June 18, 2019, with the following payment schedule: (1) an initial payment to Smart Business of $20,000; (2) daily payments to Smart Business in the amount of $2,149.50 for the period June 19, 2019, through July 3, 2019; and (3) daily payments in the amount of $4,299 until the balance of the Receivables Judgment less collection costs had been paid in full.

46. In my investigation, I have learned that on or about July 16, 2019, SYNERGY and MARESCA stopped making payments to Smart Business as required by the Forbearance Agreement leaving a balance due of approximately $283,000.

47. SYNERGY then filed its Chapter 7 bankruptcy petition in the District of Columbia one month later on August 16, 2019. SYNERGY was required as part of its Chapter 7 petition to make accurate disclosures to the bankruptcy court about SYNERGY's

assets, liabilities, and creditors. The initial bankruptcy petition signed by MARESCA included the following warning just above MARESCA's signature line: "Bankruptcy fraud is a serious crime. Making a false statement in connection with a bankruptcy case can result in fines up to $500,000 or imprisonment up to 20 years or both. 18 U.S.C. §§ 152, 1341, 1519, 3571."

48. However, SYNERGY and MARESCA willfully failed to make accurate disclosures to the bankruptcy court about the Receivables Agreement, the Receivables Judgment, and the Forbearance Agreement. On October 15, 2019, SYNERGY filed a Form 207 Statement of Financial Affairs for Non-Individuals Filing for Bankruptcy to the with the bankruptcy court in the District of Columbia. Several answers on the Form 207 were false, misleading, or fraudulent:

a. Question 1 on the form required SYNERGY to state the "gross revenue from business" the "beginning and ending dates of [SYNERGY's] fiscal year." SYNERGY stated that it had "none." That statement was false. SYNERGY plainly had gross revenues of at least $300,000 from the Receivables Agreement in the preceding year. Moreover, as discussed further below, SYNERGY had large amounts of income from payments made by victim-clients.

b. Question 2 on the form required to SYNERGY to identify any "non-business revenue" not included in its response to Question 1. SYNERGY again stated it had "none" in the prior year, even though it had collected $300,000 from the Receivables Agreement.

c. Question 3 on the form required SYNERGY to list any "payments or

transfers . . . to any creditor, other than regular employee compensation, within 90 days before filing this case unless the aggregate value of all property transferred to that creditor is less than $6,825." SYNERGY again stated "none." However, SYNERGY had paid over $40,000 to Smart Business pursuant to the Receivables Agreement and the Forbearance Agreement within the 90 days before filing for bankruptcy.

d. Question 7 on the form required SYNERGY to list any "legal actions . . . in which [SYNERGY] had been involved in any capacity . . . within 1 year before filing this case." Although SYNERGY listed a civil suit with Smart Business in New York in response, SYNERGY described the case as "pending." SYNERGY omitted any mention of the fact that Smart Business already had judgment entered against SYNERGY—the Receivables Judgment.

e. Question 13 on the form required SYNERGY to list "any transfers of money or other property … within 2 years before the filing of this case to another person" that were not listed elsewhere on the form. SYNERGY again stated "none," omitting mention again of the Receivables Agreement and the Forbearance Agreement.

Notwithstanding these false, misleading, and fraudulent answers on SYNERGY's Form 207, MARESCA declared in executing the form "under penalty of perjury that the foregoing is true and correct."

49. Based on my training and experience, MARESCA's false, misleading, an fraudulent statements to the bankruptcy court prevented the court and the parties in the SYNERGY bankruptcy case from understanding the full scope of SYNERGY's assets and liabilities; hindered the Court's ability to assess the availability of resources to make payments to all of SYNERGY's creditors; and prevented creditors from determining the actual value of their claims against SYNERGY.

TAX CRIMES

Applicable Legal Principles

50. The IRS is the component of the U.S. Department of Treasury with the lawful government function of tax administration and revenue collection. It is a violation of federal law for any person willfully to "attempt[ ] to evade or defeat any tax imposed by [the Internal Revenue Code] or the payment thereof." 26 U.S.C. § 7201. To prove that a person has committed the crime of tax evasion, the government must demonstrate three elements:

(1) Income tax was due from the defendant;

(2) The defendant attempted to evade or defeat the assessment or the payment of this tax through an affirmative act; and,

(3) The defendant acted willfully.

See generally Kevin F. O'Malley, et al., Federal Jury Practice and Instructions, Criminal § 67.03 (6th Ed.). Most commonly, the filing of a false and fraudulent return understating income is sufficient to satisfy the requirement of an attempt to evade. *Sansone v. United States*, 380 U.S. 343, 351 (1965); *United States v. Schafer*, 580 F.2d 774 (5th Cir. 1978).

But various schemes or devices may constitute tax evasion even when the defendant has failed to file a tax return.[5]

51. Any person who is required to file a tax return but willfully fails to do so also violates federal law. 26 U.S.C. § 7203.

52. For federal tax purposes, the members of a limited liability company ("LLC") have several options for assessing taxes owed to the IRS. First, an LLC can elect to be treated as a corporation and pay taxes on the LLC's income at the corporate tax rate. In order to do so, the LLC must file Form 1120 *U.S. Corporation Income Tax Return* ("Form 1120") which requires the LLC to assess and pay the taxes, if any, which are due to the IRS.

53. Second, the LLC can elect to be treated for federal tax purposes as a partnership. A partnership does not itself pay taxes, but the partners—the members of the LLC—must report the LLC's losses and income on their personal Forms 1040 *U.S. Individual Income Tax Return* ("Form 1040") and pay taxes at their individual rates. In this circumstance, the LLC must also file Form 1065 *U.S. Return of Partnership Income*

---

[5] The Supreme Court has recognized certain facts and circumstances as demonstrating an affirmative willful attempt to evade taxes:

> By way of illustration and not by way of limitation, we would think affirmative willful attempt may be inferred from conduct such as keeping a double set of books, making false entries or alterations, or false invoices or documents, destruction of books or records, concealment of assets or covering up sources of income, handling of one's affairs to avoid making the records usual in transactions of the kind, and any conduct, the likely effect of which would be to mislead or to conceal. If the tax evasion motive plays any part in such conduct, the offense may be made out even though the conduct may also serve other purposes such as the concealment of other crimes.

Spies v. United States, 317 U.S. 492, 499 (1943).

("Form 1065"), which is known as an "information return" because it provides information to the IRS about the LLC but does not assess any taxes due to the IRS.

54. Third, the LLC can elect to be treated for federal tax purposes under Subchapter S as a closely-held corporation. In general, a Subchapter S company does not pay taxes. Instead, the company's income and losses are divided among and passed through to the company's shareholders, *i.e.*, the members of the LLC. If the LLC takes this option, the LLC must file an information return, Form 1120S *U.S. Income Tax Return for an S Corporation* ("Form 1120S") with the IRS.

55. Fourth, if the LLC has only one individual member, the LLC can elect to be treated for federal tax purposes as a "disregarded entity." In this circumstance, the LLC itself does not pay taxes or make any filing with the IRS. However, the LLC individual member must report the LLC's losses and income on Schedule C of their Form 1040. The individual member will be taxed on the income generated from the business at the LLC member's individual tax rate.

Analysis of Tax Data

56. As discussed above in the bankruptcy section, MARESCA produced to the bankruptcy court on January 25, 2021, personal tax returns for tax years 2017, 2018, and 2019 that MARESCA testified that he filed with the IRS. As of April 5, 2021, the IRS has no record of receiving these tax returns. These tax returns which were self-prepared using TurboTax software were signed and dated January 8, 2021.

57. Even if these returns were in fact filed with the IRS, they vastly underreport MARESCA's true income and tax liability based on financial records subpoenaed during

the investigation and analyzed by your affiant and an FBI forensic accountant. These financial records are also corroborated by internal data maintained by the IRS.[6]

58. An analysis of MARESCA'S 2017 non-filed tax return provided to the bankruptcy court, financial records obtained via subpoenas, and internal IRS records show the following:

a. MARESCA's 2017 tax return states that MARESCA received a Form W-2 from SYNERGY ATTORNEY SERVICES ("SAS") indicating income from SAS of $105,000 with federal income tax withholdings of $18,311. The return further states that he has filed as head of household with three dependents. Overall, MARESCA alleges a tax due and owing for 2017 of $12,134 entitling MARESCA to receive a refund of $6,177.

b. MARESCA's 2017 return includes a Form Schedule C, *Profit or Loss from Business*, for SAS. MARESCA claims that for 2017 SAS incurred a $14,062 loss[7] based on gross income of $0 and expenses of $14,062.

c. The return makes no mention of SYNERGY. MARESCA has admitted that he was a 90 percent partner of SYNERGY which was formed in

---

[6] The IRS maintains copies of tax return and other financial data for all individual and non-individual filers. This data includes, for example, payments to SYNERGY and MARESCA reported by other filers; interest income earned by SYNERGY and MARESCA reported by banks; payroll records provided to the IRS; and tax return data for persons doing business with SYNERGY; and filings made by banks and casinos.

[7] This loss did not flow through to mitigate MARESCA's income.

2016. Per IRS data, MARESCA received a Form W-2 from SYNERGY for 2017 stating $36,000 of income with federal withholdings of $6,218. That income was not declared on MARESCA's return for 2017.

d. Because SYNERGY was an LLC with more than one member, SYNERGY was required for tax year 2017 to file a Form 1120 (corporation) tax return; a Form 1065 (partnership) information return; or a Form 1120S (closely held company) information return. SYNERGY made none of those filings, even though financial records that I have obtained in this investigation indicate that SYNERGY received payments of at least $1,159,488[8] from their clients in 2017.

e. But even if SYNERGY had filed an information return, MARESCA was a 90 percent owner of SYNERGY who was required to report income and losses for SYNERGY on Schedule C of his 2017 individual tax return. But MARESCA failed to report any of that data on his return for 2017.

59. An analysis of MARESCA'S 2018 non-filed tax return provided to the bankruptcy court, financial records obtained via subpoenas, and internal IRS records show the following:

a. MARESCA's 2018 tax return states that MARESCA had business income of $172,893 and gambling winnings of $58,414 with federal

[8] Per internal IRS documents, SYNERGY received $1,243,836 in payments from their credit card payment processor.

income tax withholdings of $0. Based on MARESCA's filing status of head of household and three dependents, MARESCA alleges a tax due and owing of $59,460.

b. Per internal IRS documents MARESCA had gambling winnings of $62,104 from casinos in Atlantic City, Las Vegas, and Charlestown, West Virginia.

c. MARESCA's business income is from "Consulting" on his Form Schedule C, *Profit or Loss from Business*. MARESCA claims gross income of $189,000 and expenses of $14,667 for a net profit of $172,893.

d. The return makes no mention of SYNERGY. MARESCA has admitted that he was a 90 percent partner of SYNERGY which was formed in 2016.

e. Because SYNERGY was an LLC with more than one member, SYNERGY was required for tax year 2018 to file a Form 1120, 1065, or a Form 1120S. SYNERGY made none of those filings, even though financial records that I have obtained in this investigation indicate that SYNERGY received payments of at least $5,858,073[9] from their clients in 2018.

f. But even if SYNERGY had filed an information return, MARESCA was a 90 percent owner of SYNERGY who was required to report

[9] Per internal IRS documents, SYNERGY received $6,033,279 in payments from their credit card payment processor.

income and losses for SYNERGY on Schedule C of his 2018 individual tax return. But MARESCA failed to report any of that data on his return for 2018.

60. An analysis of MARESCA'S 2019 non-filed tax return provided to the bankruptcy court, financial records obtained via subpoenas, and internal IRS records show the following:

a. MARESCA's 2019 tax return states that MARESCA had business income of $36,000 with federal income tax withholdings of $0. Based on MARESCA's filing status as head of household and three dependents, MARESCA alleges total tax liability of $4,474 with only $613 due and owing.

b. MARESCA's business income is from "Consulting" on his Form Schedule C, *Profit or Loss from Business*. MARESCA claims gross income of $36,000 and expenses of $0 for a net profit of $36,000.

c. The return makes no mention of THEMIS. MARESCA has admitted that he was a 90 percent partner of THEMIS which was formed in 2019.

d. Because THEMIS was an LLC with more than one member, THEMIS was required for tax year 2019 to file a Form 1120, 1065, or a Form 1120S. SYNERGY made none of those filings, even though financial records that I have obtained in this investigation indicate that

SYNERGY received payments of at least $1,358,381[10] from their clients in 2018.

e. But even if THEMIS had filed an information return, MARESCA was a 90 percent owner of THEMIS who was required to report income and losses for THEMIS on Schedule C of his 2019 individual tax return. But MARESCA failed to report any of that data on his return for 2019.

61. MARESCA has owned and operated SYNERGY and then THEMIS, law firms incorporated in the District of Columbia, since at least January 2017. My investigation has revealed that during the time frame 2017 through 2019, SYNERGY and THEMIS earned in aggregate more than $8.3 million of income that has never reported to the IRS.

62. The facts and circumstances discussed above support probable cause to believe that MARESCA through his entities SYNERGY then THEMIS, has willfully committed crimes in violation of federal law. MARESCA nor SYNERGY nor THEMIS have filed tax returns reflecting any income for the years 2017, 2018, and 2019, even though SYNERGY and THEMIS had more than $8.3 million in receipts during those years.

63. MARESCA is aware of tax obligations by virtue of SYNERGY and THEMIS having withdrawals and payment of employment taxes, and the companies' issuance of Forms W-2 and Forms 1099 to employees.

BOOKS, RECORDS, AND OTHER EVIDENCE

64. Every person liable for tax or who is required to file an information return

[10] At this time, investigators are still obtaining and analyzing subpoenaed financial records for THEMIS. The final income calculation may be higher.

with respect to income is required to keep permanent books of account or records, in order to establish the amount of gross income, deductions, credits, or other matters.[11] Furthermore, those books and records are required to be kept at all times available for inspection by authorized internal revenue officers or employees.[12]

65. In this case, accurate tax returns do not exist because MARESCA failed to file returns with the IRS. The best way to determine correct tax liability is to locate and examine financial books and records such as invoices, receipts, journals, and ledgers. Based on my training and experience, these books and records are likely held in hardcopy at the subject's residence and/or the business location itself, or in electronic format hosted at the business site or with a third party and accessed through a computer or other electronic device.

66. Normally, books and records in whatever format will be accessible only to business owners and store managers, often in an office filing cabinet or on a computer in an office. However, with the advancement of mobile payment platforms, these books and records may also be accessed through a mobile device or tablet that can be simultaneously used as a point of sale system in the store.

67. At this time, the format of MARESCA's books and records are believed to be QuickBooks based on MARESCA's testimony at his bankruptcy hearing.[13] However, bank records show payments from credit card payment processors, indicating that at least part of MARESCA's sales are through credit cards. In my training and experience, I know

---

[11] 26 CFR §6001(a) – Records in general

[12] 26 CFR §6001(e) – Retention of records

[13] The bankruptcy judge found MARESCA's testimony not to be credible.

that this indicates there is hardware located at the business premises to facilitate credit card purchases and keep records of such transactions.

68. Based on the forgoing, both PREMISES to be searched likely include desktop and/or laptop computers, mobile phones, and/or tablets owned, used, or controlled by MARESCA and/or employees.

PREMISES TO BE SEARCHED

69. On July 23, 2020, during a bankruptcy 341 Meeting of Creditors, MARESCA stated his home address was the RESIDENTIAL PREMISES. According to testimony provided on March 8, 2021 in the United States Bankruptcy Court, Eastern District of Virginia (Alexandria), Case No. 20-11483-KHK, MARESCA still owns the RESIDENTIAL PREMISES and still lives there.

70. Employee 1 worked at the location identified as the OFFICE PREMISES. Additionally, in approximately November or December 2020, Employee 1 was interviewed for a new position with SAS, and the interview was conducted at the OFFICE PREMISES.

71. On March 13, 2021, physical surveillance was conducted at the OFFICE PREMISES. A sign at the business park includes the names, "THEMIS LAW PLLC" and "SYNERGY STAFFING." Entryway doors on the second floor of the building are labeled, "Themis Law PLLC Suite 204" and "Themis Law PLLC Suite 201."

72. On March 18, 2021, the UCE went to the offices of THEMIS located at 8870 Rixlew Lane, Manassas, Virginia 20109 to obtain information about her loan. During the course of the UCE visit, the UCE interacted with numerous employees of THEMIS, including an employee in human resources, client relations, and legal. The employee from client relations when asked who she worked for stated THEMIS and BABBS and that all

the employees work with everybody. THEMIS assists with bankruptcies and that BABBS takes care of the bankruptcies all over the country.

73. Recent surveillance of the residence shows that MARESCA continues to occupy the property.

74. There is probable cause to believe that the books, records, and evidence described above will be found at those locations.

75. Both PREMISES are described in more detail in Attachments A1 and A2.

TECHNICAL TERMS

76. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. A "computer" means an electronic, magnetic, optical, or other high-speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

b. "Computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral

storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

c. "Mobile device" is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through "wi-fi" networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional "land line" telephones, computers, and other digital devices. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global positioning system ("GPS") locating and tracking technology, and accessing and downloading information from the Internet.

d. A "tablet" is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touchscreen. Like wireless phones, tablets function as wireless communication devices and can be used to access the

Internet or other wired or wireless devices through cellular networks, "wi-fi" networks, or otherwise. Tablets typically contain programs called applications ("apps"), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions.

e. The "Internet" is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

f. A "modem" translates signals for physical transmission to and from the ISP, which then sends and receives the information to and from other computers connected to the Internet.

g. A "router" often serves as a wireless Internet access point for one or more devices and directs traffic between computers connected to a network (whether by wire or wirelessly). A router connected to the Internet collects traffic bound for the Internet from its client machines and sends out requests on their behalf. The router also distributes to the relevant client inbound traffic arriving from the Internet. A router usually retains logs for any devices using that router for Internet connectivity. Routers, in turn, are typically connected to a modem.

h. "Encryption" is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it, but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with

the use of an encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

i. "Malware," short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware is a general term used to refer to a variety of forms of hostile or intrusive software.

COMPUTERS, ELECTRONIC/MAGNETIC STORAGE, AND FORENSIC ANALYSIS

77. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found on both PREMISES, in whatever form they are found. One form in which such items might be found is data stored on one or more digital devices. Such devices are defined above and include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard

disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

78. Thus, the warrant applied for would authorize the seizure of digital devices or, potentially, the copying of stored information, all under Rule 41(e)(2)(B). Based on my knowledge, training, and experience, as well as information provided to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that, if digital devices are found on both PREMISES, there is probable cause to believe that the items described in Attachment B will be stored in the Device(s) for at least the following reasons:

a. Individuals who engage in criminal activity, including tax evasion and structuring use digital devices

i. to house business books and records and to communicate with co-conspirators;

ii. to store on digital devices, documents and records relating to their illegal activity, which can include email correspondence; text or other "Short Message Service" ("SMS") messages; contact information of co-conspirators, including telephone numbers, email addresses, identifiers for instant messaging and social medial accounts; and records of illegal transactions, to, among other things,

1. keep track of co-conspirator's contact information;

2. keep a record of illegal transactions for future reference; and

3. keep an accounting of illegal proceeds for purposes of, among other things, splitting those proceeds with co-conspirators;

b. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often "back up" or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

c. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensics tools. When a person "deletes" a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed

Internet pages. Thus, the ability to retrieve "residue" of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer, smart phone, or other digital device habits.

79. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the digital device(s) were used, the purpose of their use, who used them (or did not), and when. Based on my knowledge, training, and experience, as well as information acquired from agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in any of the Device(s) at issue here because:

a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device(s) are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the Device(s), not currently associated with any file, can provide evidence of a file that was

once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

f. I know that when an individual uses a digital device to evade assessment of their tax liability and communicate with co-conspirators, the individual's device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain

data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense and the identities of those perpetrating it.

METHODS TO BE USED TO SEARCH DIGITAL DEVICES

80. Based on my knowledge, training, and experience, as well as information acquired from agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. Recovery of

"residue" of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting "keyword" search techniques

and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format ("PDF"), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

e. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as "AES-256 encryption" to secure and encrypt the operating system and application data, which could

only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, "Hide It Pro," disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

81. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical search of both premises.

a. Therefore, in searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

i. Upon securing the PREMISES, law enforcement personnel may, consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, seize any digital devices (that is, the Device(s)), within the scope of this warrant as defined above, deemed capable of containing the information, records, or evidence described in Attachment B and transport these items to an appropriate law enforcement laboratory or similar facility for review. For all the reasons described above, it may not be feasible to conduct a complete, safe, and appropriate search of any such digital devices at the PREMISES. The digital devices, and/or any digital images thereof created by law enforcement sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

ii. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings

it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by "opening," reviewing, or reading the images or first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "keyword" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

iii. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the seized digital devices will be specifically chosen to identify the specific items to be seized under this warrant.

iv. The seizure of the digital devices found at the PREMISES may limit the business's ability to conduct its business. As with any search warrant, I expect that this warrant will be executed reasonably. Reasonable execution will likely involve conducting an

investigation on the scene of what digital devices must be seized or copied, and what digital devices need not be seized or copied. Where appropriate, law enforcement personnel executing the warrant will copy data, rather than physically seize digital devices, to reduce the extent of disruption. If employees of the Company so request, the agents will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continuing function of the Company's legitimate business. If, after inspecting seized digital devices, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve evidence, the government will return it.

CONCLUSION

82. Based on the forgoing, I submit that there is probable cause to believe that violations have occurred of 18 U.S.C. §§ 1343 (wire fraud), 1957 (transactions with criminal proceeds); 18 U.S.C. § 157 (bankruptcy fraud); 26 U.S.C. § 7201 (attempt to evade or defeat tax); and 26 U.S.C. § 7203 (willful failure to file return, supply information, or pay tax) and that both PREMISES contains evidence of this criminal activity. Accordingly, I request that the Court issue the proposed search warrant.

Respectfully submitted,

Robert Valdini

ROBERT VALDINI
Special Agent
Internal Revenue Service, Criminal Investigation

Subscribed and sworn to in accordance
with Fed. R. Crim. P. 4.1 by telephone
on May 4, 2021:

Digitally signed by Michael S. Nachmanoff
Date: 2021.05.04 12:07:03 -04'00'

The Honorable Michael S. Nachmanoff
United States Magistrate Judge
Alexandria, Virginia